Lab Assignment 2 – Patch, Harden, Protect

Lab Write up

Based on the information above, and research from the internet, perform the following tasks:

1. List and write a brief description each of the 18 CIS Controls. (list each, and a short description of what it is)

Control 1 Inventory and Control of Enterprise Assets: This is the know your environment control. You want to a list of all things on your network and keep track of everything. You also want to monitor for anything new showing up on network scans as these may be shadow IT or malicious actors.
Control 2 Inventory and Control of Software Assets: This is like control 1 but for software. You need to be aware of what software you have in your environment to be able to remain aware of vulnerabilities that may exist in your environment. For example, if you have a piece of software and they put out a CVE for it, you need to know it's in your environment so you can take appropriate action.
Control 3 Data Protection: This is the process of identifying what data you have and if it needs to be kept or not. It is also about classifying data and putting measures to protect more sensitive data. This step also deals with disposing of data in the correct fashion. This step also covers encryption so that data at rest is protected from attackers so even if they get at the data, it will be useless to them.
Control 4 Secure Configuration of Enterprise Assets and Software: This control is about selecting and implementing a set of standardized controls from one of the many industry standards out there. You also need to continually monitor these standards for changes and may need to tweak them in the future due to new vulnerabilities as they come up.
Control 5 Account management: This control had to do with maintaining your user accounts and keeping them up to date, removing no longer active users and minimizing the number of administrative accounts in the environment. The less unused admin accounts the better. You also want to monitor for usernames and passwords that can be found online in password dumps and hove those users change their password as soon as they can. You also want to set up account monitoring and logging and monitoring for any unusual activity.
Control 6 Access Control Management: This is step is to provide tools for administering Control 5. These tools are for creating, assigning, managing, and revoking access as needed for users and others.
Control 7 Continuous Vulnerability Management: This step is all about keeping an eye on your environment with vulnerability scanners and staying up to date with the lates cyber news and CVEs to keep the window of opportunity for attackers to a minimum.
Control 8 Audit Log Management: This control is all about the way you gather and monitor audit logs from your environment. Setting up things like a SEIM to monitor and alert for certain events. This also enables log retention for post incident investigations.

Control 9 Email and Web Browser Protections: This control is where you want to implement that only approved browsers can be used in the workplace as most of these have built-in protection for known phishing sites. DNS filtering should also be used to block access to known malicious sites. For larger businesses you want to also implement DMARC to lower the chance of your users receiving spoofed emails.
Control 10 Malware Defenses: This control is about having a way to detect and control the spread of malware in a system. An example of such a program is Windows defender. For larger organizations, you may want to go with a custom EDR tool, but these are much pricier but have a lot more features for response and monitoring.
Control 11 Data Recovery: This control is all about backup. You need to determine what kind of backup schedule your business would require in the event of an incident and have sufficient back-up space for these backups. You also want to keep periodic backup isolated so that an attacker can't also encrypt your backups.
Control 12 Network Infrastructure Management: This control has to do with keeping track of all your network devices, replacing end-of-life devices and changing default configurations on network devices. You also want to keep these devices up to date as they become less secure over time.
Control 13 Network Monitoring and Defense: This control is about using tools to monitor network activity and flagging suspicious activity. This is another step where SEIM tools come in handy to monitor and alert for certain conditions. You may also want to implement network intrusion detection solutions or host base intrusion detection.
Control 14 Security Awareness and Skills Training: This control is the human element control. This is where you train your users to be able to identify phishing emails and how to handle the different types of data they may be handling. You also need to train your workforce on how to identify social engineering attacks.
Control 15 Service Provider Management: This control deals with the process of selecting a provider who will hold sensitive data or are responsible for your IT processes or platforms. Considering security, uptime, and how they handle data at rest are all important considerations. Once you select your providers it's important to keep an inventory of who they are and what they provide.
Control 16 Application Software Security: This control is for larger businesses who develop their own software or buy their own solutions from a third party. This is about always maintaining secure code or keeping on top of your provider if a vulnerability is found to remediate it. It also covers root cause analysis on security vulnerabilities to determine what caused the vulnerability.
Control 17 Incident Response Management: This Control is about establishing and maintaining an incident response plan. It also deals with training the individuals involved in and performing table-top exercises. You also want to have a way to report this information to the relevant government agencies.
Control 18 Penetration Testing: This control is about testing all the previous controls for their effectiveness. This will verify that all the work you put into securing your system has worked, or if not, will let you know where you are still vulnerable and how to best implement a fix for the issues found.

2. Which CIS Control do you think is the hardest for organizations to implement? Why?

   I think that continuous vulnerability management is one of the most difficult things to successfully implement. It is a complicated process as well as an expensive one. A successful VM program requires tools for scanning, people to run those scans, people to then prioritize and patch vulnerabilities and people to make the decision on what is important to the business as far as what mitigating factors to implement for systems that can't be patched. All these tools require proper setup as well and this is a continuous process that must be repeated on a regular basis.

3. Describe the difference between the Level 1 and Level 2 settings in the CIS benchmarks?

   The difference between Level 1 and Level 2 is level 1 is more of a minimum level of security standards and shouldn't cause any interruptions or reduce the system's functionality. Level 2 is going to be a lot more restrictive and locked down and will require micro-managing permissions and tailoring because the system has minimal permissions and will require administrative intervention a lot more than a level 1 system.

4. To familiarize yourself with the Windows 10 Enterprise Benchmarks, list the 19 recommendation categories defined in the document (HINT: The first one is Account Policies).

   1. Account Policies
   2. Local Policies
   3. Event Logs
   4. Restricted Groups
   5. Systems Services
   6. Registry
   7. File System
   8. Wired Network Policies
   9. Windows Defender Firewall with Advanced Security
   10. Network List Manager Policies
   11. Wireless Network (IEEE 802.11) Policies
   12. Public Key Policies
   13. Software Restriction Policies
   14. Network Access Protection NAP Client Configuration
   15. Application Control Policies
   16. IP Security Policies
   17. Advanced Audit Policy Configuration
   18. Administrative Templates (Computer)
   19. Administrative Templates (User)

5. To familiarize yourself with the Redhat Linux Benchmarks, list the 6

recommendation categories defined in the document (HINT: The first one is Initial Setup).

1. Initial Setup
2. Services
3. Network
4. Access, Authentication and Authorization
5. Logging and Auditing
6. System Maintenance

6. What are some similarities that you see between recommendations in the Windows 10 and Redhat Linux Benchmarks?

These recommendations have several things in common as the overall goal is the same. Both have a least privilege approach that require restricting administrative and authentication policies like password complexity, account lockout, and secure account management. Another thing they share is a focus on network security. Both recommend having host-based firewalls and secure configurations for remote access. They both also recommend removing any unused software as this will minimize the overall attach surface. Both also recommend regular system maintenance like keeping things up to date and staying up to date with the latest recommendations as these change over time.

7. What are some differences that you see between recommendations in the Windows 10 and Redhat Linux Benchmarks?

The main difference in these two benchmarks is the way they implement security controls due to the way the systems work. Windows tends to be very internal tool focused with things like group Policies, Active directory, and Windows Defender for malware protection. Whereas with Redhat uses command line tools like Sudo, sshd_config and auditd. Redhat also emphasizes package integrity verification and Kernal mode restrictions while Windows places a greater emphasis on controlling code execution through things like AppLocker and SmartScreen. The Redhat recommendations also rely more on manual configuration and scripting whereas with Windows there are more automated processes.

8. Why do you think it is important to follow common best practices like the CIS benchmarks when hardening systems?

I personally think that it is important to follow these because they are tried and tested, and no one can remember all the things covered in them every single time. It provides a way to provide a consistently secure environment and if you're following a framework there is a much lesser chance you will forget something. Another reason is for compliance reasons. If you are required to follow a framework and you are and you experience a security event then you are in the clear, you followed the rule and they just happed to be using a Zero day or something similar to bypass the established

security procedures and those where signed off by someone much higher than you more than likely. It also makes updating easier in the future if your framework pushes an update and there are only a few minor changes then all you need to do is update those few things. That is why I believe it's important to follow the framework closely.

Deliverable:

1. Gather the deliverables and lab write-up listed for each task in pdf.
2. Name the docx CTI2318-Lab2-firstname-lastname.pdf where "firstname" is your first name and "lastname" is your last name.
3. Upload to FSO in the appropriate area for Lab 2

Grading Rubric:

- ✓ **Answered all 8 questions sufficiently with Critical Thinking: 80/ 80**
- ✓ **References & Proofreading (spelling/grammar/punctuation): 10/10**
- ✓ **Followed all upload instructions: 10/10**